Anomaly Detection Report

Model: autoencoder

Source File: orglog1.csv

Total Anomalies Found: 11

Anomaly #0 | Severity: High | Type: Session Hijacking (Score: 0.0635)

```
Log Details:
syslog_ts: Jan 28 09:00:00  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 28/Jan/2026:09:00:00 +0530  request: GET /utxLogin/login HTTP/1.1  status: 302  bytes: 249  response_time: 6  referer: -  user_agent: -
```

LLM Analysis:

The anomaly in the server log indicates a potential session hijacking attack where an unauthorized user may have taken control of a valid session.

Reason for Detection:

The anomaly in the status code and the presence of a GET request for a login page with no user agent or referer information suggest a suspicious activity that could be indicative of session hijacking.

Anomaly #1 | Severity: High | Type: Data Exfiltration (Score: 0.0613)

```
Log Details:
syslog_ts: Jan 28 09:00:00  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 28/Jan/2026:09:00:00 +0530  request: GET / HTTP/1.1  status: 302  bytes: -  response_time: 1  referer: -  user_agent: -
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity.

Reason for Detection:

The anomalous features Duration and Size suggest that a large amount of data was transferred in a short period, which is indicative of data exfiltration. Additionally, the request method 'GET' and status '302' could be used to redirect data to an external domain.

Anomaly #2 | Severity: High | Type: Data Exfiltration (Score: 0.0979)

```
Log Details:
syslog_ts: Jan 27 22:51:42  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:51:42 +0530  request: GET / HTTP/1.1  status: 302  bytes: -  response_time: 0  referer: -  user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-IN) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity.

Reason for Detection:

The anomaly features Duration and Size suggest abnormal data transfer behavior, combined with a non-standard user agent 'WindowsPowerShell/5.1.26100.7462'.

Anomaly #3 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0979)

```
Log Details:
syslog_ts: Jan 27 22:51:52  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
```

Anomaly Detection Report

```
12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:51:52 +0530 request: GET / HTTP/1.1 status: 302 bytes: - response_time: 0 referer: - user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent accessing the server.

Reason for Detection:

The anomaly features Duration, Size, and Method_POST suggest abnormal behavior in the user agent Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462.

Anomaly #4 | Severity: High | Type: Data Exfiltration (Score: 0.0613)

```
Log Details:
syslog_ts: Jan 27 22:51:52 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:51:52 +0530 request: GET /utxHomeApp/redirectToHome HTTP/1.1 status: 302 bytes: - response_time: 1 referer: - user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity.

Reason for Detection:

The unusually low response time (1ms) for a request with a 302 status code, along with the anomalous features Duration: 0.0310 and Size: 0.0215, suggest that data may have been quickly extracted from the server.

Anomaly #5 | Severity: High | Type: Data Exfiltration (Score: 0.0979)

```
Log Details:
syslog_ts: Jan 27 22:51:56 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:51:56 +0530 request: GET / HTTP/1.1 status: 302 bytes: - response_time: 0 referer: - user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity.

Reason for Detection:

The unusually low response time (0) combined with the anomalous features of duration and size suggest that data may have been quickly extracted from the server.

Anomaly #6 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0613)

```
Log Details:
syslog_ts: Jan 24 14:14:28 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 24/Jan/2026:14:14:28 +0530 request: GET /boardwebapp/company/ HTTP/1.1 status: 302 bytes: - response_time: 1 referer: - user_agent: curl/8.4.0
```

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent 'curl/8.4.0'.

Reason for Detection:

The anomaly detection model flagged this log entry due to the unusual user agent 'curl/8.4.0' which could indicate a malicious intent or unauthorized access attempt.

Anomaly #7 | Severity: Medium | Type: Redirect Anomaly (Score: 0.0613)

Anomaly Detection Report

Log Details:

syslog_ts: Jan 27 22:52:41 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:52:41 +0530 request: GET /utxHomeApp/redirectToHome HTTP/1.1 status: 302 bytes: - response_time: 1 referer: - user_agent: -

LLM Analysis:

Potential redirection attack detected

Reason for Detection:

The anomaly in the server log indicates a redirect to a different domain with a response time of 1 second, which is suspicious behavior and could be indicative of a redirection attack.

Anomaly #8 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0158)

Log Details:

syslog_ts: Jan 24 14:23:26 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 24/Jan/2026:14:23:26 +0530 request: GET /agmipad/ HTTP/1.1 status: 302 bytes: - response_time: 13 referer: - user_agent: curl/8.4.0

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent activity.

Reason for Detection:

The user agent 'curl/8.4.0' in the log entry is not a common user agent for regular web browsing, which raises suspicion of a potential malicious intent.

Anomaly #9 | Severity: High | Type: Directory Traversal (Score: 0.0021)

Log Details:

syslog_ts: Jan 28 12:52:40 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 559541 domain: projectcommercials-uat.test.company.net apache_ts: 28/Jan/2026:12:52:39 +0530 request: GET /pAccounting/appResources/js/angular/controller/fcm/fcmSupportController.js?v=/../../../../../../../../bin/id%00| HTTP/1.1 status: 200 bytes: 2202 response_time: 1148 referer: https://projectcommercials-uat.test.company.net/pAccounting/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0

LLM Analysis:

The anomaly in the request field indicates a potential Directory Traversal attack where the attacker is trying to access sensitive system files by manipulating the file path.

Reason for Detection:

The presence of multiple '../' in the request field along with the null byte (%00) suggests an attempt to access files outside the web root directory, which is a common technique used in Directory Traversal attacks.

Anomaly #10 | Severity: High | Type: Directory Traversal (Score: 0.0006)

Log Details:

syslog_ts: Jan 28 12:40:35 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 559541 domain: projectcommercials-uat.test.company.net apache_ts: 28/Jan/2026:12:40:35 +0530 request: GET /pAccounting/extResources/tooltip/tipsy-docs.js?v=/..//..//..//..//..//..//..//..//..//..//..///etc/passwd%00 HTTP/1.1 status: 200 bytes: 931 response_time: 5 referer: https://projectcommercials-uat.test.company.net/pAccounting/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0

LLM Analysis:

The server log anomaly indicates a potential Directory Traversal attack where the attacker attempted to access sensitive system files by manipulating the file path in the request.

Anomaly Detection Report

Reason for Detection:

The request 'GET /pAccounting/extResources/tooltip/tipsy-docs.js?v=/../..//../../..//../../..//../../..//../../..////etc/passwd%00 HTTP/1.1' contains multiple '../' sequences which is a common technique used in Directory Traversal attacks.
